

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

LUIS ANGEL ACERO ACERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN)
YOPAL
2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

LUIS ANGEL ACERO ACERO

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Tutor:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN)
YOPAL
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Yopal, 20 de mayo de 2020

Dedico este trabajo a la universidad de la UNAD por el conocimiento que me ha impartido para ser una mejor persona y desarrollarme como profesional.

AGRADECIMIENTOS

Deseo expresar mi agradecimiento al director de este diplomado de profundización Ing. Juan Carlos Vesga y al tutor Ing. Diego Édison Ramírez por el acompañamiento que han brindado en el transcurso del curso de profundización Cisco.

CONTENIDO

	Pág.
1. RESUMEN	10
2. INTRODUCCIÓN	11
3. OBJETIVOS	12
3.1 OBJETIVO GENERAL.....	12
3.2 OBJETIVOS ESPECÍFICOS	12
4. ESCENARIO 1.....	13
4.1 ESCENARIO	13
4.2 TOPOLOGÍA	13
4.3 Parte 1: Inicializar dispositivos.....	14
4.3.1 Paso 1: Inicializar y volver a cargar los routers y los switches	14
4.4 Parte 2: Configurar los parámetros básicos de los dispositivos.....	15
4.4.1 Paso 1: Configurar la computadora de Internet	15
4.4.2 Paso 2: Configurar R1	15
4.4.3 Paso 3: Configurar R2	17
4.4.4 Paso 4: Configurar R3	19
4.4.5 Paso 5: Configurar S1	21
4.4.6 Paso 6: Configurar S3	22
4.4.7 Paso 7: Verificar la conectividad de la red	23
4.5 Parte 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN	23
4.5.1 Paso 1: Configurar S1	23
4.5.2 Paso 2: Configurar S3	25
4.5.3 Paso 3: Configurar R1	27
4.5.4 Paso 4: Verificar la conectividad de la red	28
4.6 Parte 4: Configurar el protocolo de routing dinámico RIPv2	29
4.6.1 Paso 1: Configurar RIPv2 en el R1	29
4.6.2 Paso 2: Configurar RIPv2 en el R2.....	30
4.6.3 Paso 3: Configurar RIPv2 en el R3.....	31

4.6.4 Paso 4: Verificar la información de RIPv2	31
4.7. Parte 5: Implementar DHCP y NAT para IPv4	32
4.7.1 Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 2332	32
4.7.2 Paso 2: Configurar la NAT estática y dinámica en el R2	33
4.7.3 Paso 3: Verificar el protocolo DHCP y la NAT estática	34
4.8. Parte 6: Configurar NTP	37
4.9. Parte 7: Configurar y verificar las listas de control de acceso (ACL)	37
4.9.1. Paso 1: Restringir el acceso a las líneas VTY en el R2	37
4.9.2. Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	39
5. ESCENARIO 2	41
5.1 ESCENARIO	41
5.2 TOPOLOGÍA	41
5.3 Desarrollo	43
5.3.1 Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).	43
5.3.2 Realizar la conexión física de los equipos con base en la topología de red	43
5.4 Parte 1: Configuración del enrutamiento	49
5.5 Parte 2: Tabla de Enrutamiento	52
5.6 Parte 3: Deshabilitar la propagación del protocolo OSPF	56
5.7 Parte 4: Verificación del protocolo OSPF.	56
5.8 Parte 5: Configurar encapsulamiento y autenticación PPP.	57
5.9 Parte 6: Configuración de PAT.	59
5.10 Parte 7: Configuración del servicio DHCP.	60
CONCLUSIONES	63
BIBLIOGRAFÍA	64

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento.....	14
Tabla 2. Inicialización y cargue de los routers y switches.....	14
Tabla 3. Configuración del servidor de internet.....	15
Tabla 4. Configuración R1	15
Tabla 5. Configuración R2	17
Tabla 6. Configuración R3	19
Tabla 7. Configuración S1	21
Tabla 8. Configuración S3	22
Tabla 9. Verificar conectividad de la red	23
Tabla 10. Configuración S1	24
Tabla 11. Configuración S3	26
Tabla 12. Configuración R1	27
Tabla 13. Verificar la conectividad de la red	28
Tabla 14. Configurar RIPv2 en R1	29
Tabla 15. Configurar RIPv2 en R2	30
Tabla 16. Configurar RIPv2 en R3	31
Tabla 17. Verificar la información de RIPv2.....	31
Tabla 18. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	32
Tabla 19. Configurar la NAT estática y dinámica en el R2.....	33
Tabla 20. Verificar el protocolo DHCP y la NAT estática	34
Tabla 21. Configurar NTP	37
Tabla 22. Restringir el acceso a las líneas VTY en el R2	37
Tabla 23. Introducir el comando de CLI para ACL	39
Tabla 24. Direcciones IP por Redes	42
Tabla 25. Direcciones IP por Redes	42
Tabla 26. Sumarización Red Medellín	52
Tabla 27. Sumarización Red Bogotá	52
Tabla 28. Interfaces de cada router que no necesitan desactivación	56

LISTA DE FIGURAS

Figura 1. Topología de red.....	13
Figura 2. Verificación exitosa de conectividad S1	28
Figura 3. Verificación exitosa de conectividad S3.....	29
Figura 4. Verificación DHCP PC-A.....	35
Figura 5. Verificación DHCP PC-C	35
Figura 6. Verificación ping PC-A a PC-C	36
Figura 7. Verificación de acceso al servidor web desde navegador web PC-A	36
Figura 8. Verificación de clock de R1.....	37
Figura 9. Verificación exitosa de acceso desde R1 a R2.....	38
Figura 10. Verificación fallida de acceso de R3 a R2.....	38
Figura 11. Verificación ping desde PC-A	39
Figura 12. Topología de red.....	41
Figura 13. Diagrama de Red.....	48
Figura 14. Estado de la red, Redes directamente conectadas a Medellin1	48
Figura 15. Estado de la red, Redes directamente conectadas a Bogotá1	48
Figura 16. tabla de rutas Medellín 1	53
Figura 17. tabla de rutas Medellín 2.....	53
Figura 18. Tabla de rutas Medellín 3	53
Figura 19. Tabla de rutas Bogotá 1	54
Figura 20. Tabla de rutas Bogotá 2.....	54
Figura 21. Tabla de rutas Bogotá 3.....	54
Figura 22. ISP solo muestra las rutas estáticas y las conectadas directamente....	55
Figura 23. Rutas OSPF red Medellín	57
Figura 24. Rutas OSPF Red Bogotá.....	57
Figura 25. ping entre ISP y medellin1 y viceversa	58
Figura 26. Verificación de asignación DHCP en los PC de la red Medellín	61
Figura 27. Verificación de asignación DHCP en los PC de la red Bogotá	62

1. RESUMEN

En este proyecto se lleva a la practica el conocimiento adquirido en el diplomado de profundización cisco sobre diseño e implementación de soluciones integradas lan y wan, haciendo simulaciones en el programa de Cisco Packet Tracer sobre dos escenarios diferentes, donde se crean topologías físicas y se analizan diferentes redes configurando los dispositivos de red según los requerimientos de cada escenario. Se evidenciará la documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante el desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

2. INTRODUCCIÓN

Como base fundamental en desarrollo académico como próximos ingenieros de sistemas, la UNAD en convenio con CISCO Networking Academy, han puesto a disposición el diplomado: “diplomado de profundización cisco (diseño e implementación de soluciones integradas lan / wan)”, donde se encuentra dos módulos, CCNA Routing and Switching: Introducción a redes, donde brinda la capacidad al estudiante de construir redes LAN simples, realizar configuraciones básicas para enrutadores e interruptores, e implementar esquemas de direccionamiento IP, el segundo Routing y switching de CCNA: Principios básicos de routing y switching, donde se presenta herramientas para configurar y solucionar problemas de enrutadores y cambia y resuelve problemas comunes con RIPv1, RIPv2, área única y área múltiple OSPF, LAN virtuales y enrutamiento entre VLAN en ambas redes IPv4 e IPv6, como evaluación se desarrolla la prueba de habilidades prácticas en este documento en la que el estudiante que demuestra las habilidades desarrolladas.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado poniendo a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

3.2 OBJETIVOS ESPECÍFICOS

- Configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.
- Configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

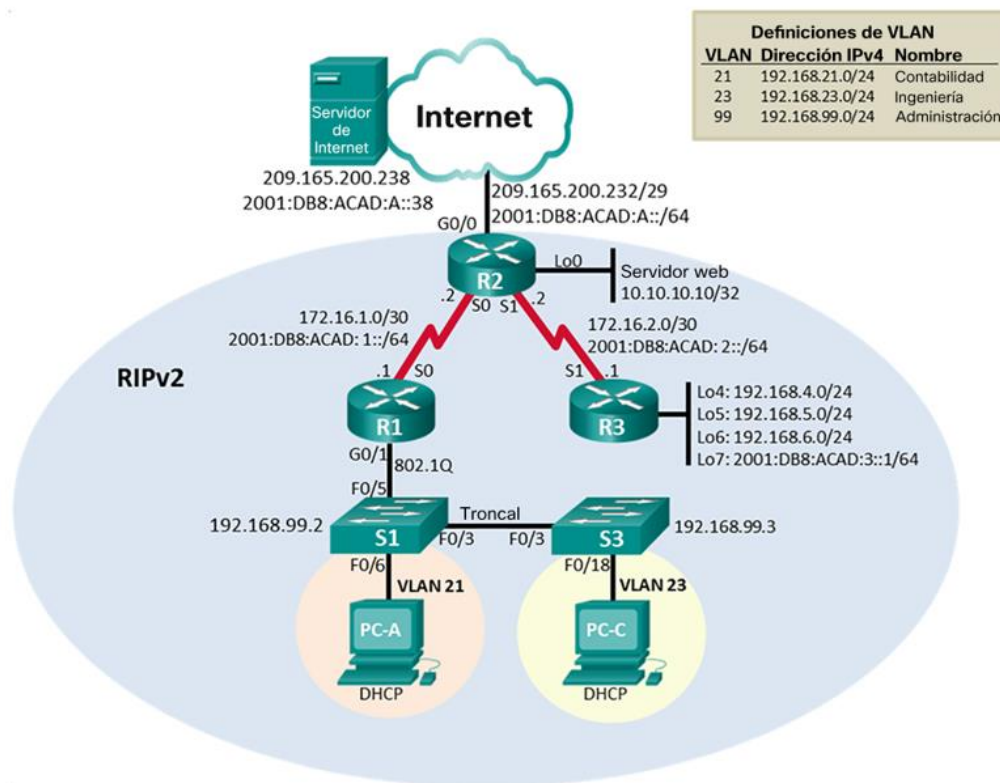
4. ESCENARIO 1

4.1 ESCENARIO

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

4.2 TOPOLOGÍA

Figura 1. Topología de red



Link Drive de Pkt Escenario 1:

https://drive.google.com/file/d/1qvO5I7XYKaU_eR5tiOArgS2cYCrwxR32/view?usp=sharing

Tabla 1. Tabla de direccionamiento.

EQUIPO	PUERTO	DIRECCIÓN IP	IPV6	MASCARA	ENLACE
R1	S0/1/0	172.16.1.1	2001:DB8:ACAD:1::1/64	255.255.255.252	R2
	G0/0/1.21	192.168.21.1		255.255.255.0	S1
	G0/0/1.23	192.168.23.1		255.255.255.0	S1
	G0/0/1.99	192.168.99.1		255.255.255.0	S3
R2	S0/1/0	172.16.1.2	2001:DB8:ACAD:1::2/64	255.255.255.252	R2
	S0/1/1	172.16.2.2	2001:DB8:ACAD:2::2/64	255.255.255.252	R3
	G0/0/0	209.165.200.225	2001:DB8:ACAD:A::1/64	255.255.255.248	Servidor
	LO0	10.10.10.10.		255.255.255.255	Servidor web
R3	S0/1/1	172.16.2.1	2001:DB8:ACAD:2::1/64	255.255.255.252	R2
	Lo4	192.168.4.1		255.255.255.0	Lo4
	Lo5	192.168.5.1		255.255.255.0	Lo5
	Lo6	192.168.6.1		255.255.255.0	Lo6
	Lo7		2001:DB8:ACAD:3::1/64		Lo7
S1	Vlan99	192.168.99.2		255.255.255.0	
	Vlan21	192.168.21.2		255.255.255.0	
S3	Vlan99	192.168.99.3		255.255.255.0	
	Vlan23	192.168.23.1		255.255.255.0	
PC-A	G0/0/0	DHCP			
PC-B	G0/0/0	DHCP			

4.3 Parte 1: Inicializar dispositivos

4.3.1 Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 2. Inicialización y cargue de los routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	erase startup-config delete flash:vlan.dat
Volver a cargar ambos switches	Reload
Verificar que la base de datos de	Show vlan

VLAN no esté en la memoria flash en ambos switches	
--	--

4.4 Parte 2: Configurar los parámetros básicos de los dispositivos

4.4.1 Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 3. Configuración del servidor de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.168.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

4.4.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Nota: Todavía no configure G0/1

Configuración del Router

```

Router>enable
Router#configure terminal
Router(config)#Hostname R1
R1(config)#Enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd !Se prohíbe el acceso no autorizado !

```

Configuración de los puertos seriales entre R1 y R2

```

R1(config)#interface serial 0/1/0
R1(config-if)#description R1-R2
R1(config-if)#clock rate 128000
R1(config-if)#ip address 173.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#no shutdown

```


Configuración Ruta Estática

R1(config-if)#ipv6 Route 2001:DB8:ACAD:1::1/64 2001:DB8:ACAD:4::1

R1(config)#ip route 0.0.0.0 0.0.0.0 S0/1/0

4.4.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 5. Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	Se configura en el servidor
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	<p>Establecer la descripción.</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p>
Interfaz loopback 0 (servidor web simulado)	<p>Establecer la descripción.</p> <p>Establezca la dirección IPv4.</p>
Ruta predeterminada	<p>Configure una ruta IPv4 predeterminada de G0/0.</p> <p>Configure una ruta IPv6 predeterminada de G0/0.</p>

Configuración de router

```

Router>enable
Router#configure terminal
Router(config)#Hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd !Se prohíbe el acceso no autorizado!
Configuración de R2 A R1
R2(config)#interface serial 0/1/0
R2(config-if)#description R2-R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#No shutdown

```

Configuración de R2 A R3

```

R2(config)#Interface serial 0/1/1
R2(config-if)#Description R2-R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252

```

```
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
```

Configuración R2 – Servidor

```
R2(config)#interface gigabit 0/0/0
R2(config-if)#description R2-Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown
R2(config-if)#end
```

Configuración R2- WEB server

```
R2(config)#interface lo0
R2(config-if)#description R2-Web Server
R2(config-if)#ip address 10.10.10.10 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Configuración Rutas Estáticas

```
R2(config-if)#ip route 0.0.0.0 0.0.0.0 Gigabit0/0/0
R2(config)#ipv6 route 2001:DB8:ACAD:A::1/64 2001:DB8:ACAD:A::2
R2(config)#end
R2#
```

4.4.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 6. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class

Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Configuración del Router

```

Router>enable
Router#configure terminal
Router(config)#Hostname R3
R3(config)#no ip domain-lookup
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit

```

```
R3(config)#service password-encryption
R3(config)#banner motd !Prohibido el acceso no autorizado!
```

Configuración Puerto R3-R2

```
R3(config)#Interface serial 0/1/1
R3(config-if)#Description R3-R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3 (config-if)#no shutdown
```

Configuración de las Looback

```
R3(config)#interface lo4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface lo5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface lo6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface lo7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#EXIT
R3(config)#
```

4.4.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 7. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco

Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Configuración de Switch

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#Hostname S1

S1(config)#enable secret class

S1(config)#line console 0

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#line vty 0 4

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#service password-encryption

S1(config)#banner motd !Prohibido el Acceso no Autorizado!

S1(config)#exit

4.4.6 Paso 6: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 8. Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption

Mensaje MOTD	Se prohíbe el acceso no autorizado.
--------------	-------------------------------------

Configuración de Switch

```
Switch>enable
Switch#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#Hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#Line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #Prohibido el Acceso No Autorizado#
S3(config)#exit
```

4.4.7 Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 9. Verificar conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.238	Satisfactorio

4.5 Parte 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

4.5.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 10. Configuración S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	S1(config)#interface fast 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#
Apagar todos los puertos sin usar	S1(config)#interface range fast 0/6-24 S1(config-if-range)#shut

Creacion de Vlan

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#vlan 21

S1(config-vlan)#Name Contabilidad

S1(config-vlan)#exit

S1(config)#Vlan 23

S1(config-vlan)#Name Ingenieria

S1(config-vlan)#exit

S1(config)#vlan 99

S1(config-vlan)#name Administracion

S1(config-vlan)#exit

S1(config)#

Asignación de ip a vlan y gateway predeterminado

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.21.1
S1(config)#end
```

Configuración de Interfaces fastEthernet 5 y 3

```
S1(config)#interface fas 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#end
S1(config)#interface fas 0/3
S1(config-if)#switchport mode trunk
switchport trunk native vlan 1
S1(config-if)#end
S1#
```

Configuración de puertos modo Access

```
S1(config)#interface range fast 0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 1
S1(config-if-range)#end
```

```
S1(config)#interface range fast 0/6-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 1
S1(config-if-range)#end
```

4.5.2 Paso 2: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 11. Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

```

S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#exit
S3(config)#vlan 23
S3(config-vlan)#Name Ingenieria
S3(config-vlan)#exit
S3(config)#Vlan 99
S3(config-vlan)#Name Administracion
S3(config-vlan)#EXIT
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.23.1
S3(config)#interface fas0/3
S3(config-if)#siswitchport mode trunk
S3(config-if)#shswitchport trunk native vlan 1
S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2

```

```

S3(config-if-range)#switchport mode access
S3(config-if-range)#shut
S3(config)#interface fas 0/18
S3(config-if)# switchport mode access
S3(config-if)#switchport access vlan 23
S3(config)default-gateway 192.168.23.1

```

4.5.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12. Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Comandos usados en la configuración de la interfaz

```

R1(config)#interface Gigabit 0/0/1.21
R1(config-subif)#Description Contabilidad_LAN
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface Gigabit 0/0/1.23
R1(config-subif)#Description Ingenieria_LAN
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0

```

```

R1(config-subif)#exit
R1(config)#interface Gigabit 0/0/1.99
R1(config-subif)#Description Administracion_LAN
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface Gigabit 0/0/1
R1(config-if)#no shutdown

```

4.5.4 Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio 5/5
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio 5/5
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio 5/5
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio 5/5

Figura 2. Verificación exitosa de conectividad S1

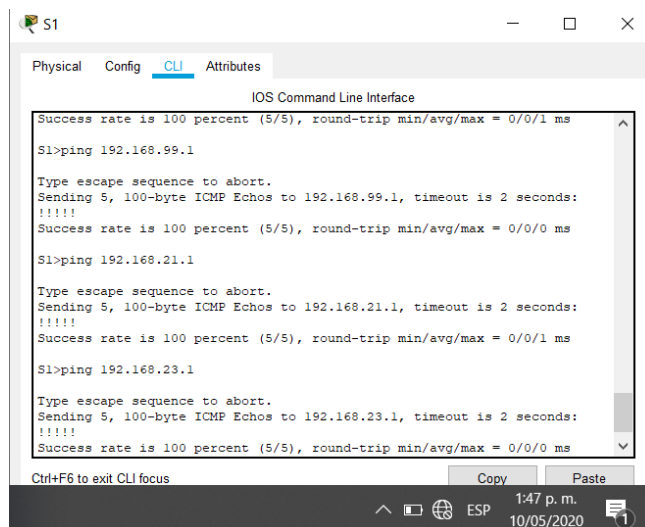
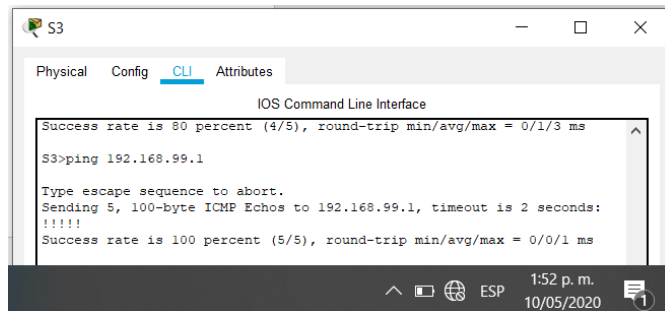


Figura 3. Verificación exitosa de conectividad S3



4.6 Parte 4: Configurar el protocolo de routing dinámico RIPv2

4.6.1 Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configurar RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Comandos Usados en la configuración

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 172.16.1.0

R1(config-router)#network 192.168.21.0

R1(config-router)#network 192.168.23.0

R1(config-router)#network 192.168.99.0

R1(config-router)#passive-interface gigabit0/0/1

R1(config-router)#no auto-summary

Configuración RIP con IPV6

R1(config)#ipv6 unicast-routing

```

R1(config)#ipv6 router rip CISCO
R1(config-rtr)#interface serial 0/1/0
R1(config-if)#ipv6 rip CISCO enable
R1(config-if)#
R1#

```

4.6.2 Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 15. Configurar RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Comandos usados en la configuración

```

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#network 10.10.10.0
R2(config-router)#passive-interface lo0
R2(config-router)#no auto-summary
R2(config-router)#end

```

Configuración RIP IPV6

```

R2(config)#ipv6 unicast-routing
R2(config)#ipv6 router rip CISCO
R2(config-rtr)#interface Serial 0/1/0
R2(config-if)#ipv6 rip CISCO enable
R2(config-if)#interface Serial 0/1/1
R2(config-if)#ipv6 rip CISCO enable
R2(config-if)#end

```

4.6.3 Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 16. Configurar RIPv2 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

```
R3#config t
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#no auto-summary
R3(config-router)#end
```

4.6.4 Paso 4: Verificar la información de RIPv2

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 17. Verificar la información de RIPv2

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas RIP?	show ip route rip

¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show running-config
--	---------------------

4.7. Parte 5: Implementar DHCP y NAT para IPv4

4.7.1 Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

R1(config)#ip dhcp pool ACCT

R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#ip domain-name ccna-sa.com

R1(config)#ip dhcp pool ACCT

R1(dhcp-config)#default-router 192.168.21.1

R1(dhcp-config)#network 192.168.21.0 255.255.255.0


```

R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#ip domain-name ccna-sa.com

```

4.7.2 Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	

```

R2(config)#user userweb privilege 15 secret cisco
R2(config)#ip http server
R2(config)#ip http secure-server
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.99.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface gigabit 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#interface serial 0/1/0
R2(config-if)#ip nat inside
R2(config-if)#interface serial 0/1/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
R2#

```

4.7.3 Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 20. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio

<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	Satisfactorio
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	La computadora de internet no hace parte del diagrama guía presentado por el Tutor en la presenta guía

Figura 4. Verificación DHCP PC-A

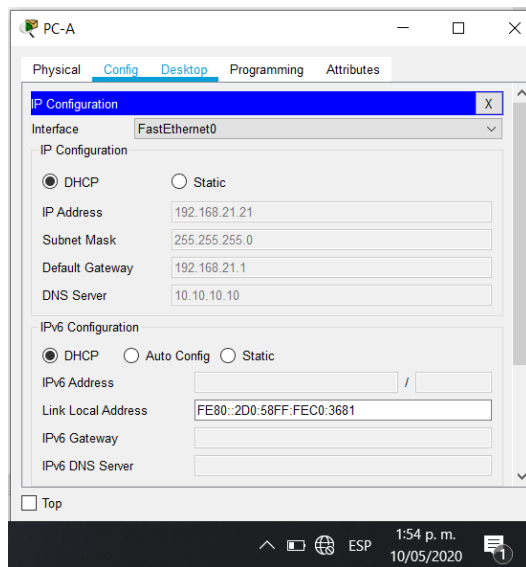


Figura 5. Verificación DHCP PC-C

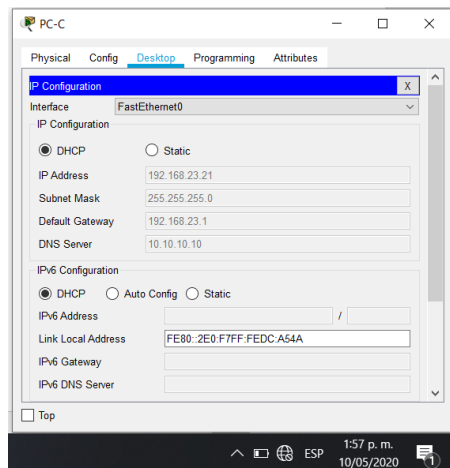


Figura 6. Verificación ping PC-A a PC-C

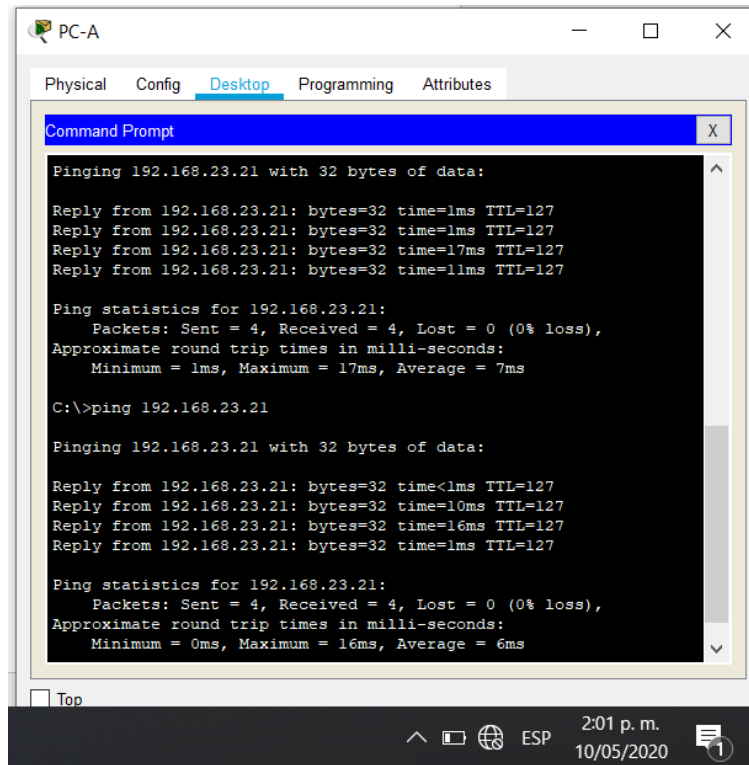
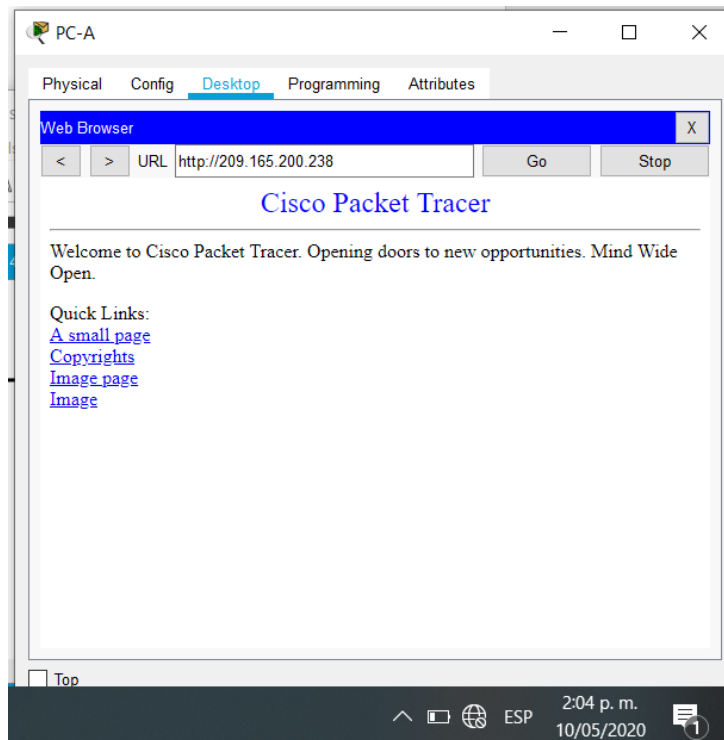


Figura 7. Verificación de acceso al servidor web desde navegador web PC-A



4.8. Parte 6: Configurar NTP

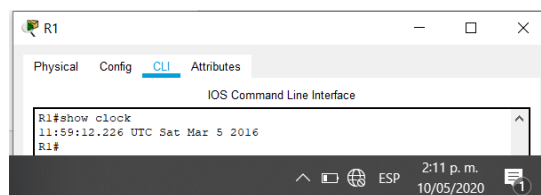
Tabla 21. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

```
R2#clock set 09:00:00 mar 5 2016
R2#config t
R2(config)#ntp master 5
```

```
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#
```

Figura 8. Verificación de clock de R1



4.9. Parte 7: Configurar y verificar las listas de control de acceso (ACL)

4.9.1. Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 22. Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT

Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ip access-list standard ADMIN-MGT

R2(config-std-nacl)#permit host 172.16.1.1

R2(config-std-nacl)#exit

R2(config)#line vty 0 4

R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#exit

R2(config)#

Las siguientes imágenes muestran el correcto funcionamiento de la lista de accesos

Figura 9. Verificación exitosa de acceso desde R1 a R2

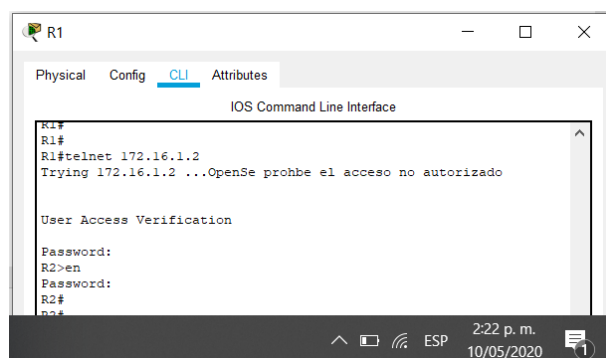


Figura 10. Verificación fallida de acceso de R3 a R2

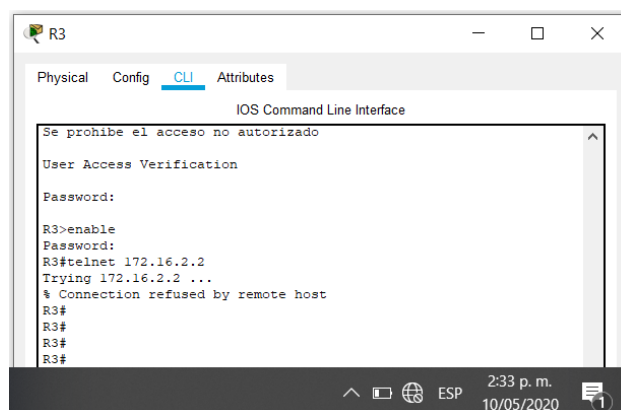
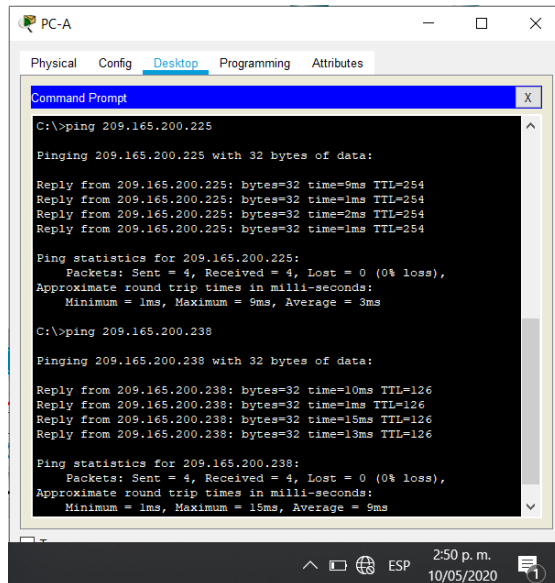


Figura 11. Verificación ping desde PC-A



Al realizar este procedimiento se pierde la conexión de los pc con el servidor web por lo que se debe configurar en R2 una lista de acceso para que permita el acceso de estos host al servidor, el código usado es el siguiente:

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 100 permit tcp any host 209.165.200.225 eq www
R2(config)#access-list 100 permit icmp any any echo-reply
R2(config)#interface gigabit 0/0/0
R2(config-if)#ip access-group 100 in
R2(config-if)#exit
  
```

4.9.2. Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 23. Introducir el comando de CLI para ACL

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list

Restablecer los contadores de una lista de acceso	Clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip access-lists
¿Con qué comando se muestran las traducciones NAT?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation para eliminar las traducciones NAT

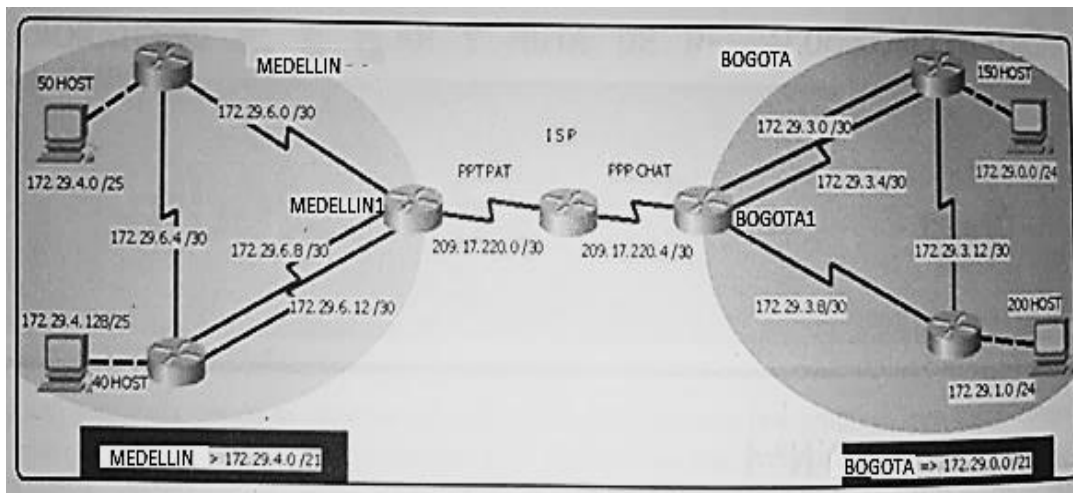
5. ESCENARIO 2

5.1 ESCENARIO

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

5.2 TOPOLOGÍA

Figura 12. Topología de red



Link Drive de Pkt Escenario 2:

https://drive.google.com/file/d/15KN9gHAeHvNjcfvMLhpag7hVIWIWz_5F/view?usp=sharing

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1

Tabla 24. Direcciones IP por Redes

Nombre de la red	IP de la red	Mascara de la red	Wildcard	Host o subredes
Medellin 1 - Medellin 2	172.29.6.0	255.255.255.252 = 30	0.0.0.3	172.29.6.1 - 172.29.6.2
Medellin 1 - Medellin 3	172.29.6.8	255.255.255.252 = 30	0.0.0.3	172.29.6.9 - 172.29.6.10
Medellin 1 - Medellin 3	192.29.6.12	255.255.255.252 = 30	0.0.0.3	172.29.6.13 – 172.29.6.14
Medellin 2 - Medellin 3	172.29.6.4	255.255.255.252 = 30	0.0.0.3	172.29.6.5 – 172.29.6.6
ISP – Medellin	209.17.220.0	255.255.255.252 = 30	0.0.0.3	209.17.220.1 - 209.17.220.2
ISP - Bogota	209.17.220.4	255.255.255.252 = 30	0.0.0.3	209.17.220.5 - 209.17.220.6
Bogota 1 - Bogota 3	172.29.3.0	255.255.255.252 = 30	0.0.0.3	172.29.3.1 - 172.29.3.2
Bogota 1 - Bogota 3	172.29.3.4	255.255.255.252 = 30	0.0.0.3	172.29.3.5 - 172.29.3.6
Bogota 1 - Bogota 3	172.29.3.8	255.255.255.252 = 30	0.0.0.3	172.29.3.9 - 172.29.3.10
Bogota 2 – Bogota 3	172.29.3.12	255.255.255.252 = 30	0.0.0.3	172.29.3.13 - 172.29.3.14

Tabla 25. Direcciones IP por Redes

EQUIPO	PUERTO	DIRECCIÓN IP	MASCARA	ENLACE
ISP	S0/0/0	209.17.220.1	255.255.255.252	MEDELLIN1
	S0/0/1	209.17.220.5	255.255.255.252	BOGOTA1
BOGOTA1	S0/0/0	209.17.220.6	255.255.255.252	ISP
	S0/0/1	172.29.3.9	255.255.255.252	BOGOTA2
	S0/1/0	172.29.3.5	255.255.255.252	BOGOTA3
	S0/1/1	172.29.3.1	255.255.255.252	BOGOTA3
	S0/0/0	172.29.3.10	255.255.255.252	BOGOTA1
BOGOTA2	S0/0/1	172.29.3.13	255.255.255.252	BOGOTA3
	G0/0	172.29.1.1	255.255.255.0	PC-200 HOST
PC-200 HOST	G0/0	172.29.1.2	255.255.255.0	BOGOTA2
BOGOTA3	S0/0/0	172.29.3.2	255.255.255.252	BOGOTA1
	S0/0/1	172.29.3.6	255.255.255.252	BOGOTA1
	S0/1/0	172.29.3.14	255.255.255.252	BOGOTA2
	F0/0	172.29.0.1	255.255.255.0	PC-150 HOST
PC-150 HOST	F0/0	172.29.0.2	255.255.255.0	BOGOTA3
MEDELLIN1	S0/0/0	172.29.6.1	255.255.255.252	MEDELLIN2
	S0/0/1	172.29.6.9	255.255.255.252	MEDELLIN3
	S0/1/0	172.29.6.13	255.255.255.252	MEDELLIN3
	S0/1/1	209.17.220.2	255.255.255.252	ISP
MEDELLIN2	S0/0/0	172.29.6.2	255.255.255.252	MEDELLIN1
	S0/0/1	172.29.6.5	255.255.255.252	MEDELLIN3
	G0/0	172.29.4.1	255.255.255.128	PC-50 HOST
PC-50 HOST	G0/0	172.29.4.2	255.255.255.128	
MEDELLIN3	S0/0/0	172.29.6.6	255.255.255.252	MEDELLIN2
	S0/0/1	172.29.6.10	255.255.255.252	MEDELLIN1
	S0/1/0	172.29.6.14	255.255.255.252	MEDELLIN1
	G0/1/1	172.29.4.129	255.255.255.128	PC-40
PC-50 HOST	G0/0/0	172.29.4.130	255.255.255.128	MEDELLIN3

5.3 Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

5.3.1 Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Para la configuración básica de los Router se usan los siguientes comandos realizando la adecuación de según el router

```
enable
Configure Terminal
hostname ISP (Se debe modificar de acuerdo al Router que se quiera configurar)
No ip domain-lookup
Line console 0
Password cisco
Login
Logging synchronous
Exit
Line vty 0 15
Password cisco
Login
Exit
Enable password class
Service password-encryption
banner motd # Solo personal autorizado #
exit
copy running-config startup-config
```

5.3.2 Realizar la conexión física de los equipos con base en la topología de red

Se realiza la configuración lógica y física de la red

Configuración de la ISP

Aunque la guía no lo solicita por funcionar como ISP se configura el clock rate con el máximo valor posible y se apagan los puertos que no se usaran

```
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#Interface serial 0/1/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown
ISP(config-if)#exit
```

```
ISP(config)#Interface serial 0/1/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown
```

```
ISP#conf t
ISP(config)#interface range gigabit 0/0/0-2
ISP(config-if-range)#shutdown
ISP(config-if-range)#end
```

Configuración de Medellin1

```
Medellin1(config)#enable
Medellin1(config)#configure terminal
Medellin1(config)#interface serial 0/1/0
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/1/1
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 4000000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/2/0
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 4000000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/2/1
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 4000000
Medellin1(config-if)#no shutdown
```

```
Medellin1(config-if)#exit
Medellin1(config)#interface range gigabit 0/0/0-2
Medellin1(config-if-range)#shutdown
Medellin1(config-if-range)#end
```

Configuración de Medellin2

```
Medellin2#configure terminal
Medellin2(config)#interface serial 0/1/0
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#interface serial 0/1/1
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 4000000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#interface Gigabit 0/0/0
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#interface range gigabit 0/0/1-2
Medellin2(config-if-range)#shutdown
Medellin2(config-if-range)#
```

Configuración de Medellin3

```
Medellin3#configure terminal
Medellin3(config)#interface serial 0/1/0
Medellin3(config-if)#ip address 172.26.6.6 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface serial 0/2/0
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface serial 0/2/1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface Gigabit 0/0/0
```

```
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface range gigabit 0/0/1-2
Medellin3(config-if-range)#shutdown
Medellin3(config)#interface range serial 0/1/1
Medellin3(config-if-range)#shutdown
```

Configuración Bogota1

```
Bogota1#configure terminal
Bogota1(config)#interface serial 0/1/0
Bogota1(config-if)#ip address 209.17.225.6 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/1/1
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 4000000
Bogota1(config-if)#No shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/2/0
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 4000000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/2/1
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 4000000
Bogota1(config-if)#no shut
Bogota1(config-if)#exit
Bogota1(config)#interface range gigabit 0/0/0-2
Bogota1(config-if-range)#no shutdown
Configurar la topología de red, de acuerdo con las siguientes especificaciones.
```

Configuración Bogota2

```
Bogota2#configure terminal
Bogota2(config)#interface serial 0/1/0
Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota2(config-if)#No shutdown
Bogota2(config-if)#exit
```

```
Bogota2(config)#interface serial 0/1/1
Bogota2(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota2(config-if)#clock rate 4000000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface gigabit 0/0/0
Bogota2(config-if)#ip address 172.29.1.1 255.255.255.128
Bogota2(config-if)#no shutdwon
Bogota2(config-if)#exit
Bogota2(config)#interface range gigabit 0/0/1-2
Bogota2(config-if-range)#shutdown
```

Configuración Bogota3

```
Bogota3#configure terminal
Bogota3(config)#interface serial 0/1/0
Bogota3(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#interface serial 0/1/1
Bogota3(config-if)#shut
Bogota3(config-if)#exit
Bogota3(config)#interface serial 0/2/0
Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#interface serial 0/2/1
Bogota3(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#interface gigabit 0/0/0
Bogota3(config-if)#ip address 172.29.0.1 255.255.255.128
Bogota3(config-if)#no shut
Bogota3(config-if)#exit
Bogota3(config)#interface range gigabit 0/1/0-2
interface range not validated - command rejected
```

Figura 13. Diagrama de Red

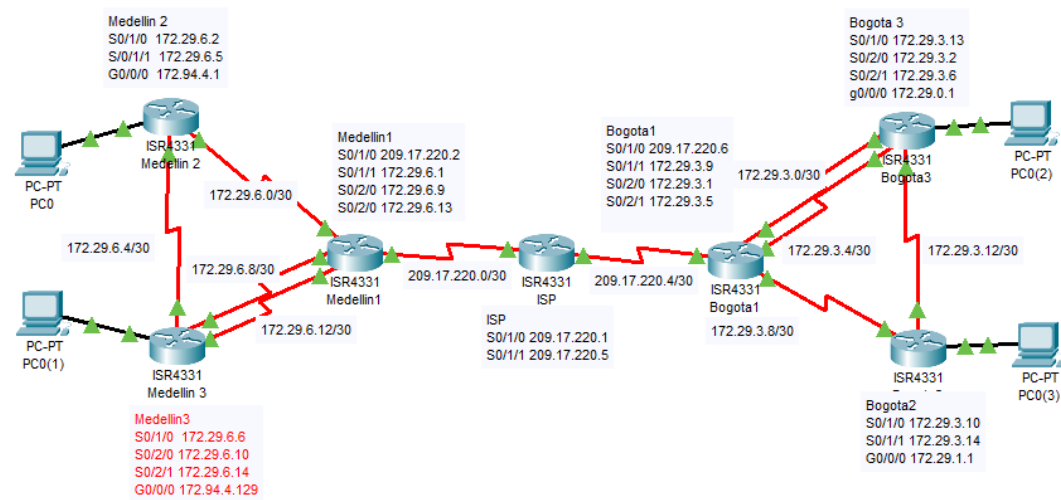


Figura 14. Estado de la red, Redes directamente conectadas a Medellin1

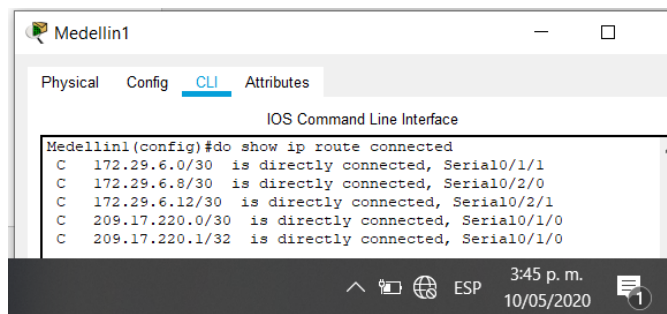
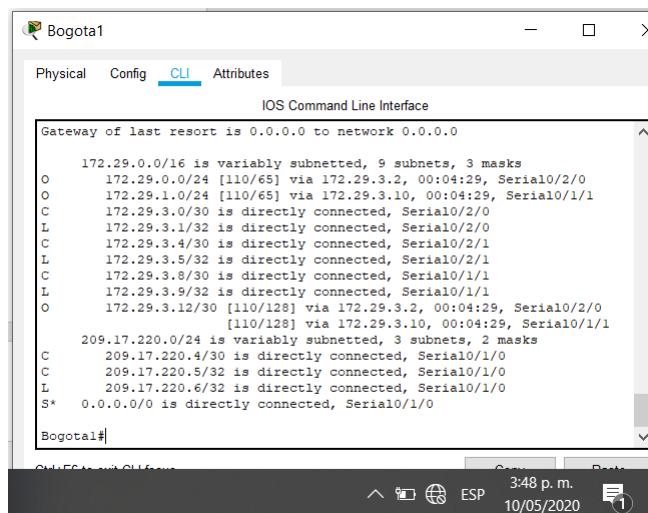


Figura 15. Estado de la red, Redes directamente conectadas a Bogota1



5.4 Parte 1: Configuración del enrutamiento

- a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática. (Dado que OSPF no resume automáticamente, lo necesita el comando auto-summary)
- b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Medellin1#configure terminal

(Se verifica las rutas que se conectan directamente al router)

Medellin1(config)#do show ip route connected

C 172.29.6.0/30 is directly connected, Serial0/1/1

C 172.29.6.8/30 is directly connected, Serial0/2/0

C 172.29.6.12/30 is directly connected, Serial0/2/1

C 209.17.220.0/30 is directly connected, Serial0/1/0

Se configura OSPF

Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

Medellin1(config)#Router ospf 1

Medellin1(config-router)#Router-id 1.1.1.1

Medellin1(config-router)#network 17.29.6.0 0.0.0.3 area 0

Medellin1(config-router)#network 17.29.6.8 0.0.0.3 area 0

Medellin1(config-router)#network 17.29.6.12 0.0.0.3 area 0

Medellin1(config-router)#passive-interface s0/1/0

Medellin1(config-router)#default-information originate

Medellin1(config-router)#exit

Medellin1(config)#exit

Medellin2

Medellin2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Medellin2(config)#do show ip route connected

C 172.29.6.0/30 is directly connected, Serial0/1/0

C 172.29.6.4/30 is directly connected, Serial0/1/1

C 172.94.4.0/25 is directly connected, GigabitEthernet0/0/0

Medellin2(config)#Router ospf 1

```
Medellin2(config-router)#Router-id 2.2.2.2
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#passive-interface G0/0/0
Medellin2(config-router)#exit
Medellin2(config)#exit
Medellin2#
```

Medellin3

```
Medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/2/1
C 172.29.6.12/30 is directly connected, Serial0/2/0
```

```
Medellin3(config)#Router ospf 1
Medellin3(config-router)#Router-id 3.3.3.3
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#passive-interface g0/0/0
Medellin3(config-router)#end
Medellin3#
```

Bogota1

```
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/2/0
C 172.29.3.4/30 is directly connected, Serial0/2/1
C 172.29.3.8/30 is directly connected, Serial0/1/1
C 209.17.225.4/30 is directly connected, Serial0/1/0

Bogota1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0
Bogota1(config)#Router ospf 1
```

```
Bogota1(config-router)#router-id 1.1.1.1
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota1(config-router)#passive-interface serial 0/1/0
Bogota1(config-router)#default-information originate
Bogota1(config-router)#end
```

Bogota2

```
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#do show ip route connected
C 172.29.1.0/25 is directly connected, GigabitEthernet0/0/0
C 172.29.3.8/30 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/1/1
```

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#router-id 2.2.2.2
Bogota2(config-router)#network 172.29.1.0 0.0.0.255 area 1
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 1
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 1
Bogota2(config-router)#passive-interface g0/0/0
Bogota2(config-router)#end
```

Bogota3

```
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#do show ip route connected
C 172.29.0.0/25 is directly connected, GigabitEthernet0/0/0
C 172.29.3.0/30 is directly connected, Serial0/2/0
C 172.29.3.4/30 is directly connected, Serial0/2/1
C 172.29.3.12/30 is directly connected, Serial0/1/0
```

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#router-id 3.3.3.3
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 1
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 1
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 1
```

```
Bogota3(config-router)#passive-interface g0/0/0
Bogota3(config-router)#end
```

c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarian las subredes de cada uno a /22.

Para realizar una correcta sumariación de las redes se hace necesario hacer conversión a binario para ello se trabajará con la siguiente tabla

Tabla 26. Sumarización Red Medellín

MEDELLIN			128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
172.29.4.0	172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
172.29.4.128	172	29	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
172.29.6.0	172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
172.29.6.12	172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0
172.29.6.8	172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0
172.29.6.4	172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0
172.29.4.0	172	29	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0

Tabla 27. Sumarización Red Bogotá

BOGOTA			128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
172.29.1.0	172	29	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
172.29.3.0	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
172.29.0.0	172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
172.29.3.8	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0
172.29.3.4	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0
172.29.3.12	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0
172.29.0.0	172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

```
ISP#config t
ISP(config)#ip route 172.29.4.0 255.255.252.0 Serial 0/1/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

5.5 Parte 2: Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Figura 16. tabla de rutas Medellín 1

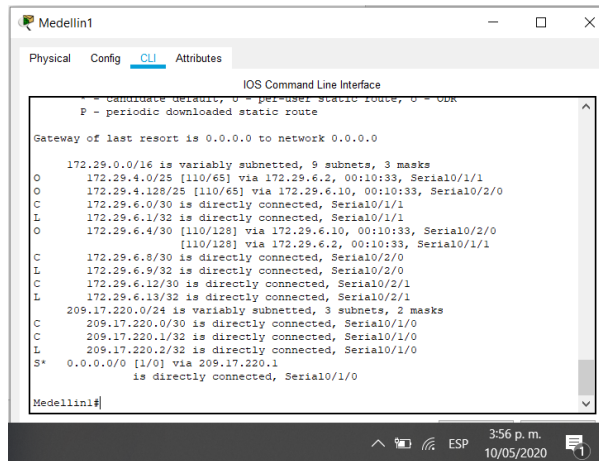


Figura 17. tabla de rutas Medellín 2

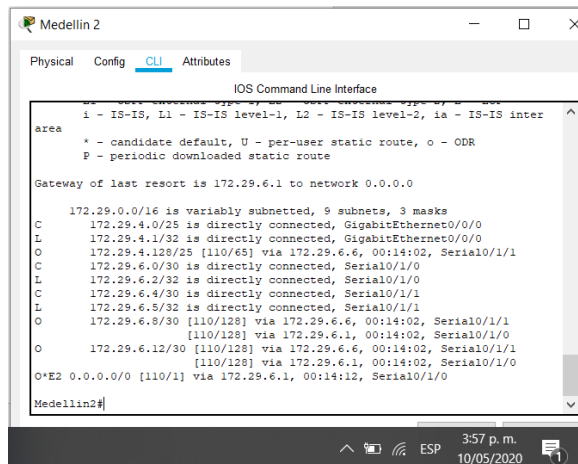


Figura 18. Tabla de rutas Medellín 3

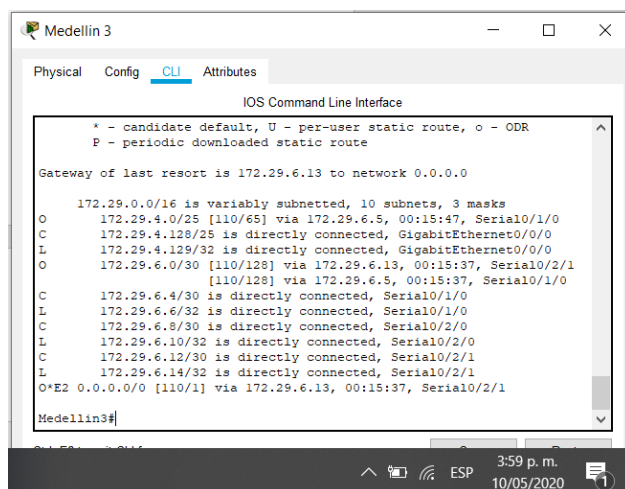


Figura 19. Tabla de rutas Bogotá 1

```

Bogota1
Physical Config CLI Attributes
IOS Command Line Interface
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.0.0/24 [110/65] via 172.29.3.2, 00:17:32, Serial0/2/0
O 172.29.1.0/24 [110/65] via 172.29.3.10, 00:17:32, Serial0/1/1
C 172.29.3.0/30 is directly connected, Serial0/2/0
L 172.29.3.1/32 is directly connected, Serial0/2/0
C 172.29.3.4/30 is directly connected, Serial0/2/1
L 172.29.3.5/32 is directly connected, Serial0/2/1
C 172.29.3.8/30 is directly connected, Serial0/1/1
L 172.29.3.9/32 is directly connected, Serial0/1/1
O 172.29.3.12/30 [110/128] via 172.29.3.2, 00:17:32, Serial0/2/0
  [110/128] via 172.29.3.10, 00:17:32, Serial0/1/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C 209.17.220.4/30 is directly connected, Serial0/1/0
C 209.17.220.5/32 is directly connected, Serial0/1/0
L 209.17.220.6/32 is directly connected, Serial0/1/0
S* 0.0.0.0/0 is directly connected, Serial0/1/0
Bogota1#
  
```

Figura 20. Tabla de rutas Bogotá 2

```

Bogota2
Physical Config CLI Attributes
IOS Command Line Interface
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.3.9 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.0.0/24 [110/65] via 172.29.3.13, 00:18:32, Serial0/1/1
O 172.29.1.0/24 is directly connected, GigabitEthernet0/0/0
L 172.29.1.1/32 is directly connected, GigabitEthernet0/0/0
O 172.29.3.0/30 [110/128] via 172.29.3.13, 00:18:32, Serial0/1/1
  [110/128] via 172.29.3.9, 00:18:32, Serial0/1/0
O 172.29.3.4/30 [110/128] via 172.29.3.13, 00:18:32, Serial0/1/1
  [110/128] via 172.29.3.9, 00:18:32, Serial0/1/0
C 172.29.3.8/30 is directly connected, Serial0/1/0
L 172.29.3.10/32 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/1/1
L 172.29.3.14/32 is directly connected, Serial0/1/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:18:42, Serial0/1/0
Bogota2#
  
```

Figura 21. Tabla de rutas Bogotá 3

```

Bogota3
Physical Config CLI Attributes
IOS Command Line Interface
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0/0
L 172.29.0.1/32 is directly connected, GigabitEthernet0/0/0
O 172.29.1.0/24 [110/65] via 172.29.3.14, 00:19:39, Serial0/1/0
C 172.29.3.0/30 is directly connected, Serial0/2/0
L 172.29.3.2/32 is directly connected, Serial0/2/0
C 172.29.3.4/30 is directly connected, Serial0/2/1
L 172.29.3.6/32 is directly connected, Serial0/2/1
O 172.29.3.8/30 [110/128] via 172.29.3.1, 00:19:39, Serial0/2/0
  [110/128] via 172.29.3.14, 00:19:39, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/1/0
L 172.29.3.13/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:19:39, Serial0/2/0
Bogota3#
  
```

b. Verificar el balanceo de carga que presentan los routers.

Cada router Posee dos rutas posibles para llegar a las redes lejanas esto se puede observar en las imágenes del punto anterior donde se ven las rutas de los equipos

c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Los router con el mismo numero tienen una tabla de ruta muy similar, dada la estructura de redundante de las redes bogota y medellin bogota1 y medellin1 tienen similitud, esta similitud tambien se puede observar en los dispositivos de frontera (Bogata2-Medellin2, Bogota3-Medellin3)

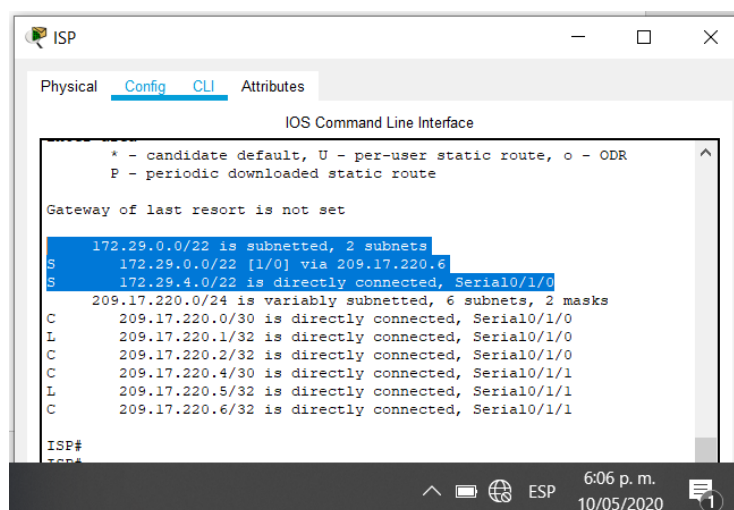
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Las imágenes aportadas en el inciso a se observan las rutas redundantes de cada uno de los routers.

f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Figura 22. ISP solo muestra las rutas estáticas y las conectadas directamente.



5.6 Parte 3: Deshabilitar la propagación del protocolo OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 28. Interfaces de cada router que no necesitan desactivación

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Este paso se realizó con antelación teniendo en cuenta que los puertos que no son usados fueron apagados por consola esto para el caso de los puertos Gigabit Y serial en cada Router.

5.7 Parte 4: Verificación del protocolo OSPF.

a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Este paso se realizó cuando se configuro OSPF en cada uno de los routers y se dejó las interfaces Gigabit que conectan los PC como pasivas y en caso de los router que conecta con la ISP en cada una de las redes el puerto serial 0/1/0 se dejó pasivo

b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Figura 23. Rutas OSPF red Medellín

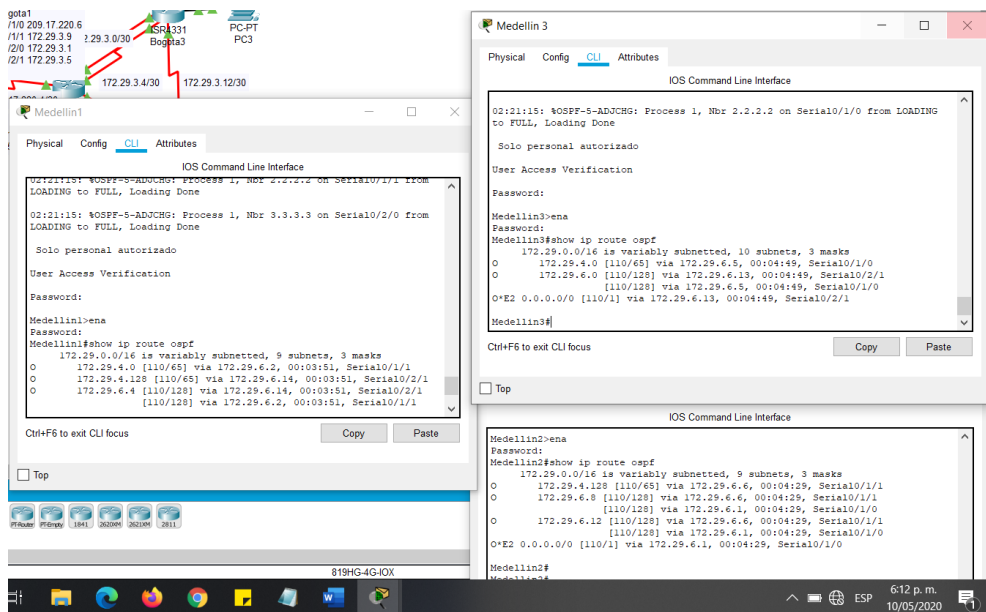
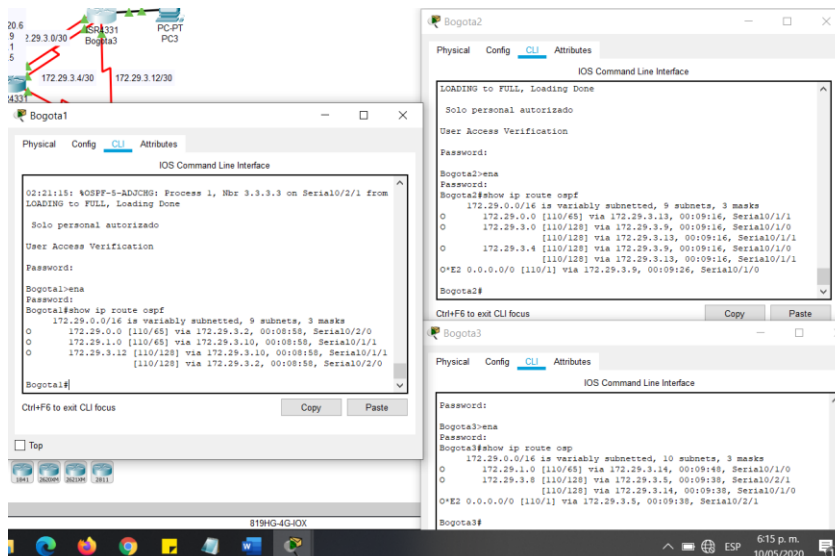


Figura 24. Rutas OSPF Red Bogotá



5.8 Parte 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

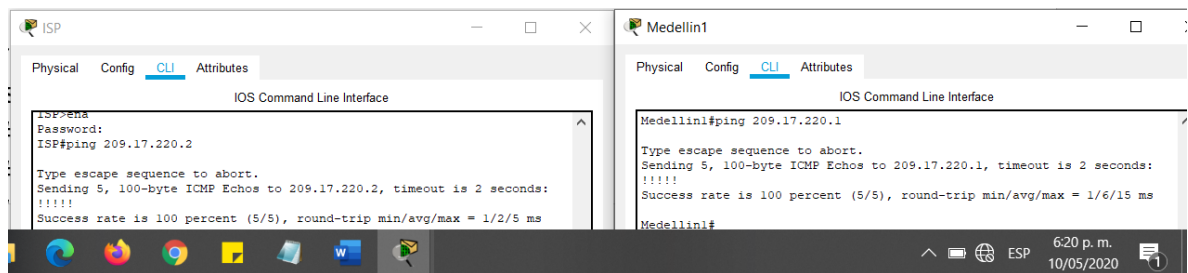
ISP#Configure Terminal

ISP(config)#username Medellin1 password cisco123

```
ISP(config)#interface serial 0/1/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco123
ISP(config-if)#end
```

```
Medellin1#configure terminal
Medellin1(config)#username ISP password cisco123
Medellin1(config)#interface Serial 0/1/0
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin1 password cisco123
Medellin1(config-if)#end
```

Figura 25. ping entre ISP y medellin1 y viceversa



b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

```
ISP#config terminal
ISP(config)#username Bogota1 password cisco123
ISP(config-if)#int s0/1/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
```

```
Bogota1#conf t
Bogota1(config)#username ISP password cisco123
Bogota1(config)#interface s 0/1/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#end
Bogota1#
```

5.9 Parte 6: Configuración de PAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
- b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, como diferente puerto.

```
Medellin1#configure terminal
Medellin1(config)#ip nat inside source list 1 interface serial 0/1/0 overload
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config)#interface serial 0/1/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/1/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/2/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/2/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#end
Medellin1#
```

- c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, como diferente puerto.

```
Bogota1#config t
Bogota1(config)#ip nat inside source list 1 interface s0/1/0 overload
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota1(config)#int s0/1/0
```

```

Bogota1(config-if)#ip nat outside
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/2/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/2/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#

```

5.10 Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

```

Medellin2#configure terminal
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.6
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.135
Medellin2(config)#ip dhcp pool Medellin2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#dns-server 8.8.4.4
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool Medellin3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#dns-server 8.8.4.4
Medellin2(dhcp-config)#exit
Medellin2(config)#

```

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

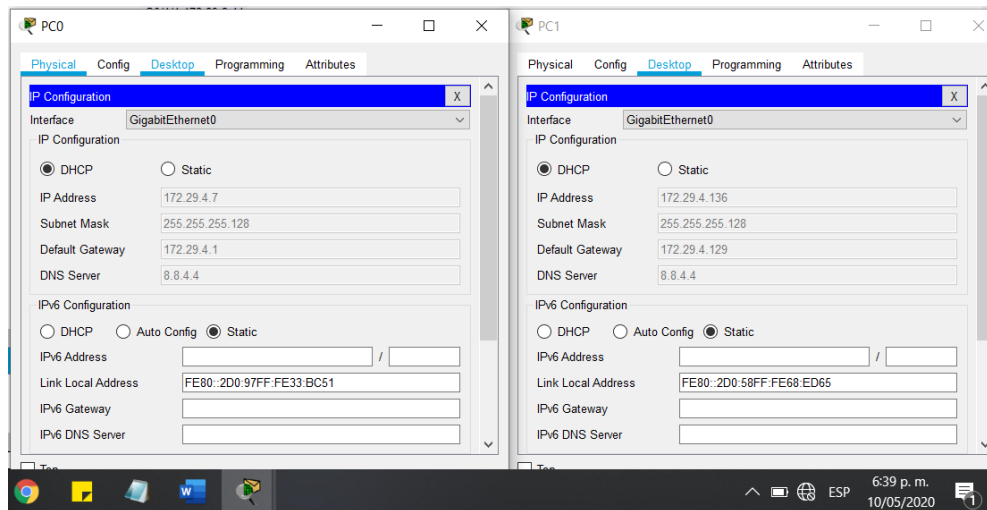
```

Medellin3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#Interface G0/0/0
Medellin3(config-if)#ip helper-address 172.29.6.5

```

Medellin3(config-if)#end

Figura 26. Verificación de asignación DHCP en los PC de la red Medellín



c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

Los que pide el punto es inviable por lo que se asume un error de digitación por parte del docente y se procede a configurar

Bogota2#Configure terminal

Bogota2(config)# ip dhcp excluded-address 172.29.1.1 172.29.1.8

Bogota2(config)# ip dhcp excluded-address 172.29.0.1 172.29.0.8

Bogota2(config)# ip dhcp pool Bogota2

Bogota2(dhcp-config)# network 172.29.1.0 255.255.255.0

Bogota2(dhcp-config)# default-router 172.29.1.1

Bogota2(dhcp-config)# dns-server 8.8.8.8

Bogota2(dhcp-config)# exit

Bogota2(config)# ip dhcp pool Bogota3

Bogota2(dhcp-config)# network 172.29.0.0 255.255.255.0

Bogota2(dhcp-config)# default-router 172.29.0.1

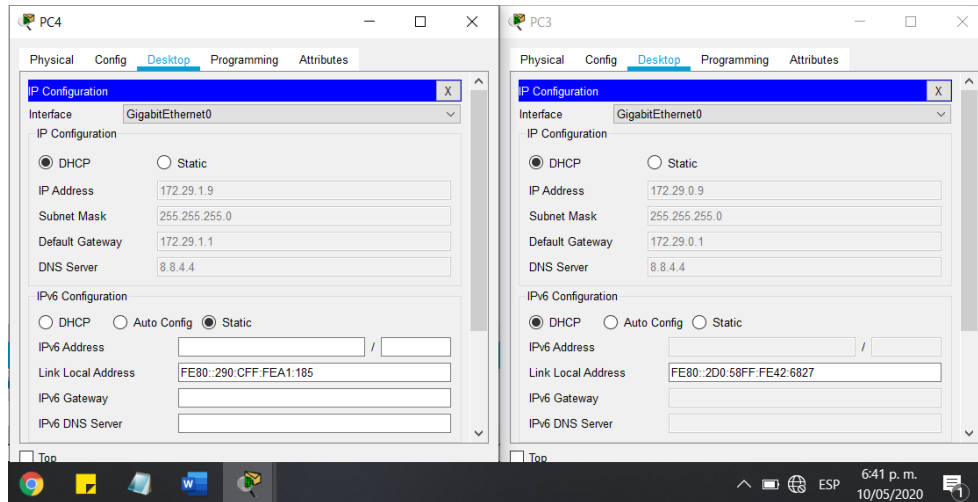
Bogota2(dhcp-config)# dns-server 8.8.8.8

Bogota2(dhcp-config)# end

d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
Bogota3#configure terminal
Bogota3(config)#interface g0/0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
Bogota3(config)#end
Bogota3#
```

Figura 27. Verificación de asignación DHCP en los PC de la red Bogotá



CONCLUSIONES

Al finalizar la actividad se pudo establecer la topología e inicializar los dispositivos, configurar los parámetros requeridos a los dispositivos y verificar la conectividad, configurar rutas y verificar la conectividad, configurar IPv6 y verificar la conectividad, verificar la configuración predeterminada y se configuraron las VLAN.

Una red se puede dividir en subredes, y esa subred se puede subdividir nuevamente. Este proceso se puede repetir varias veces para crear subredes de distintos tamaños, según el número de hosts requerido en cada subred. Este uso es con VLSM que requiere la planificación de direcciones.

En redes LAN es importante que los dispositivos de infraestructura de red, como los switches y routers, también se configuren con características de seguridad.

Se llegó a la importancia del uso al servidor DHCP ya que es determinante cuando se va a asignar direcciones de red a una cantidad grande de computadores en vez de asignarlas manualmente, lo cual es algo eficaz en estos ámbitos.

Se entiende que el mecanismo para intercomunicar redes de distintas clases, en transportar información a través del router sin importar la clase debe usarse la NAT.

Se comprende que RIPv2 es un protocolo de routing vector distancia sin clase y RIPv6 es un protocolo de routing vector distancia para enrutar direcciones IPv6.

Con el protocolo OSPF permite hacer routing como estado de enlace en las redes IP.

BIBLIOGRAFÍA

Cisco. (2020). CP CCNA1 I-2020 16-01. Recuperado 20 abril de 2020, de <https://www.netacad.com/portal/learning>

Cisco. (2020). CP CCNA2 I-2020 16-01. Recuperado 27 abril de 2020, de <https://www.netacad.com/portal/learning>

Romero, C. (2013). 4.1.4.6 Lab - Configuración Básica de las Características de un Router con IOS CLI. Recuperado 27 abril de 2020 de <https://www.youtube.com/watch?v=ioLZLByeLEY>

Krasniqi, A. (2015). Packet Tracer 2.2.4.9 - Configuring Switch Port Security Instructions - CCNA 2 - Chapter 2. Recuperado 27 abril de 2020 de <https://www.youtube.com/watch?v=Mniom9xrd98>

Walton, A. (2018). Configuración de PAT (NAT con sobrecarga). Recuperado 27 de abril de 2020, de <https://ccnadesdecero.es/configuracion-pat-nat-sobrecarga/>

Romero, C. (2014). 7.3.2.4 Lab - Configuring Basic RIPv2 and RIPv6. Recuperado 27 abril de 2020 de https://www.youtube.com/watch?v=_0VD7mIHCEY

Romero, C. (2014). 3.3.6 Lab - Configuring Basic Single-Area OSPFv3. Recuperado 27 abril de 2020 de <https://www.youtube.com/watch?v=mAeNQG9MR9w>